FIG.1

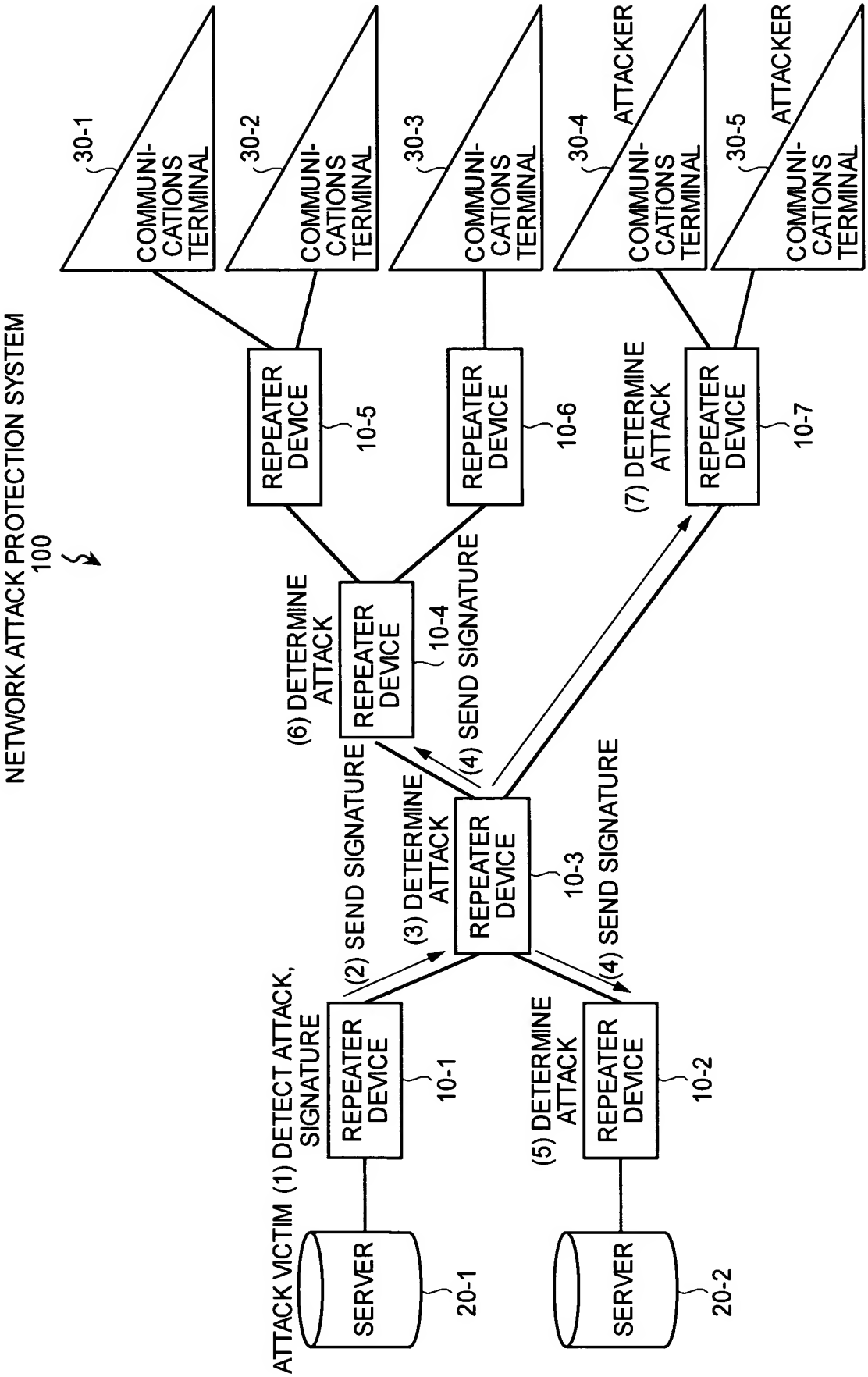

NETWORK ATTACK PROTECTION SYSTEM
100
30-1
COMMUNI-CATIONS TERMINAL
30-2
COMMUNI-CATIONS TERMINAL
30-3
COMMUNI-CATIONS TERMINAL
30-4
ATTACKER
COMMUNI-CATIONS TERMINAL
30-5
ATTACKER
COMMUNI-CATIONS TERMINAL
REPEATER DEVICE
10-5
REPEATER DEVICE
10-6
REPEATER DEVICE
10-7
(7) DETERMINE ATTACK
(6) DETERMINE ATTACK
REPEATER DEVICE
10-4
(4) SEND SIGNATURE
(2) SEND SIGNATURE
(3) DETERMINE ATTACK
REPEATER DEVICE
10-3
(4) SEND SIGNATURE
ATTACK VICTIM
(1) DETECT ATTACK, SIGNATURE
REPEATER DEVICE
10-1
(5) DETERMINE ATTACK
REPEATER DEVICE
10-2
SERVER
20-1
SERVER
20-2

FIG.2

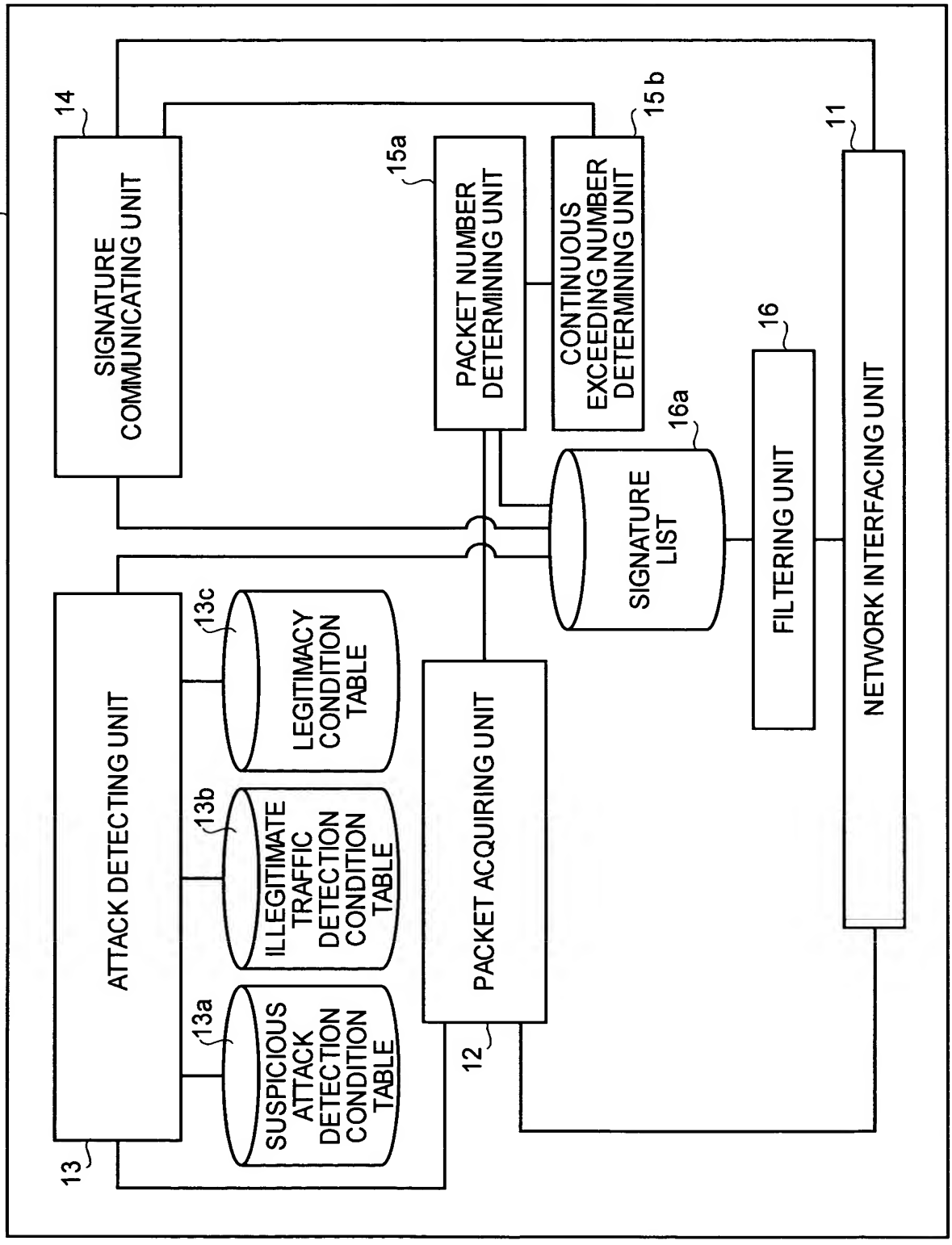

REPEATER DEVICE
10
SIGNATURE COMMUNICATING UNIT
14
PACKET NUMBER DETERMINING UNIT
15a
CONTINUOUS EXCEEDING NUMBER DETERMINING UNIT
15 b
NETWORK INTERFACING UNIT
11
SIGNATURE LIST
16a
FILTERING UNIT
16
ATTACK DETECTING UNIT
13
LEGITIMACY CONDITION TABLE
13c
ILLEGITIMATE TRAFFIC DETECTION CONDITION TABLE
13b
SUSPICIOUS ATTACK DETECTION CONDITION TABLE
13a
PACKET ACQUIRING UNIT
12

FIG.3

SUSPICIOUS ATTACK DETECTION CONDITION TABLE

13a

NO.	DETECTION ATTRIBUTES	DETECTION THRESHOLD	DETECTION TIME
1	{Dst=192.168.1.1/32,Protocol=TCP,Port=80}	500 Kbps	10 SECONDS
2	{Dst=192.168.1.2/32,Protocol=UDP}	300 Kbps	10 SECONDS
3	{Dst=192.168.1.1/24}	1000 Kbps	20 SECONDS
⋮			

FIG.4

ILLEGITIMATE TRAFFIC DETECTION CONDITION TABLE

13b

NO.	ILLEGITIMATE TRAFFIC CONDITIONS
1	PACKETS AT OR MORE ARE CONTINUOUSLY TRANSMITTED FOR S1 SECONDS OR MORE
2	ICMP/Echo Reply PACKETS AT T2 Kbps OR MORE ARE CONTINUOUSLY TRANSMITTED FOR S2 SECONDS OR MORE
3	FRAGMENT PACKETS AT T3 Kbps OR MORE ARE CONTINUOUSLY TRANSMITTED FOR S3 SECONDS OR MORE
⋮	

FIG.5

LEGITIMACY CONDITION TABLE

13c

NO.	DETECTION ATTRIBUTES
1	{Src=172.16.10.0/24}
2	{TOS=0×01}
⋮	

FIG.6

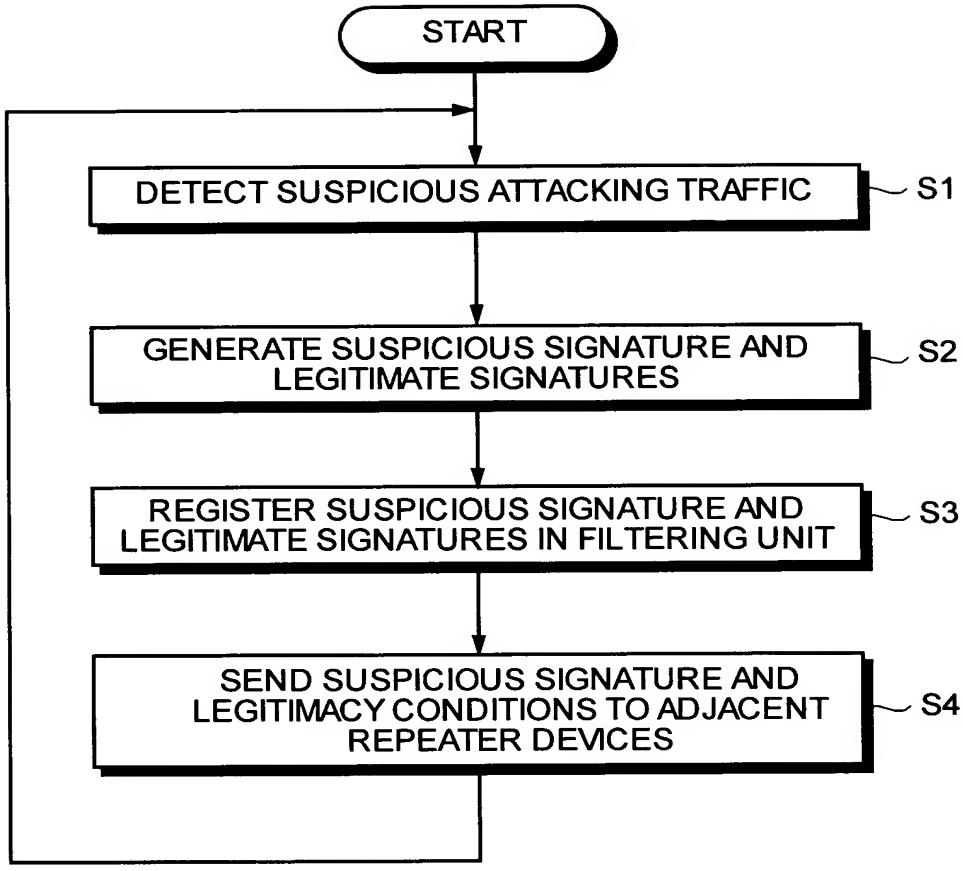

START
DETECT SUSPICIOUS ATTACKING TRAFFIC
S1
GENERATE SUSPICIOUS SIGNATURE AND LEGITIMATE SIGNATURES
S2
REGISTER SUSPICIOUS SIGNATURE AND LEGITIMATE SIGNATURES IN FILTERING UNIT
S3
SEND SUSPICIOUS SIGNATURE AND LEGITIMACY CONDITIONS TO ADJACENT REPEATER DEVICES
S4

FIG.7

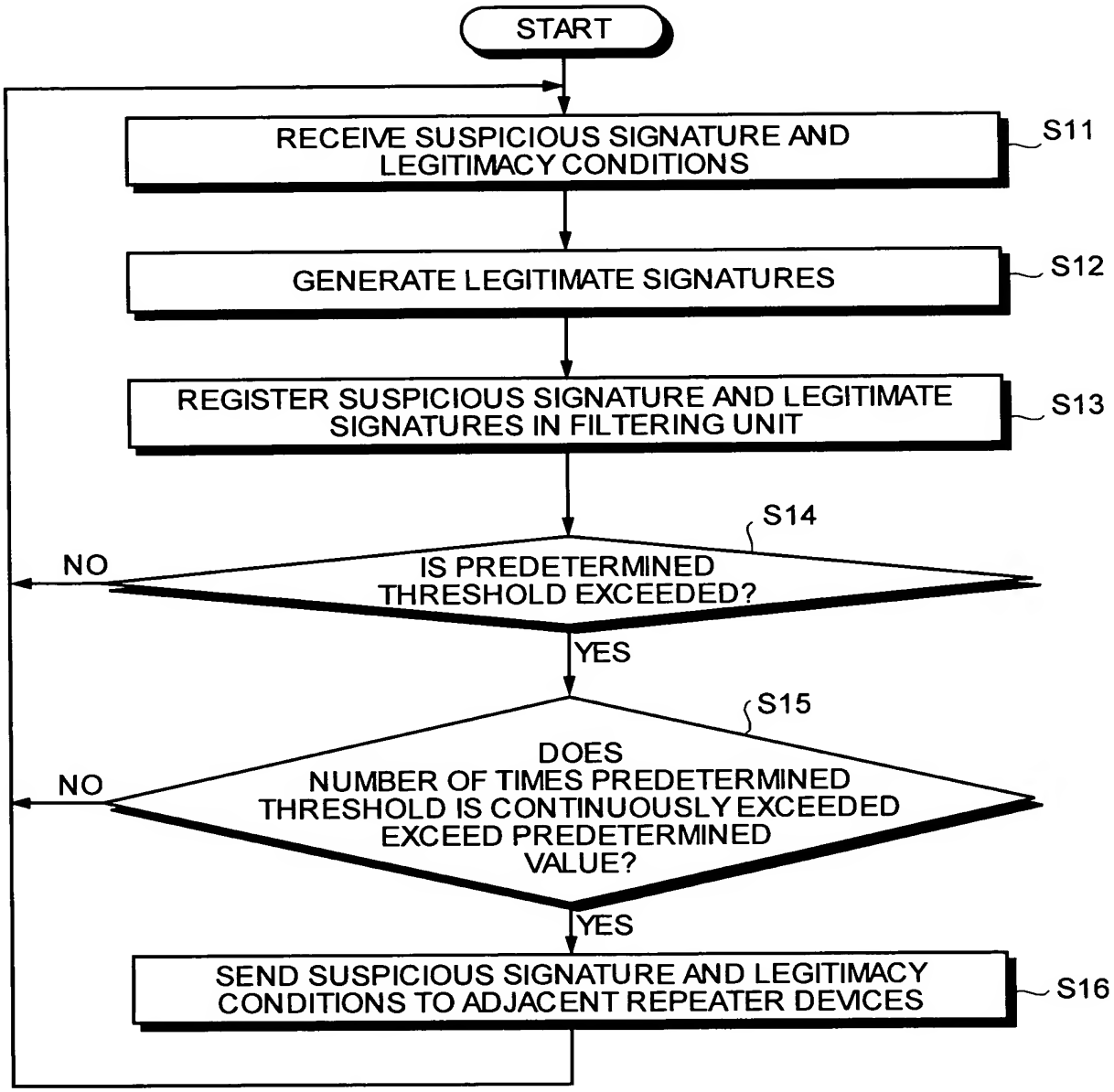

START
RECEIVE SUSPICIOUS SIGNATURE AND LEGITIMACY CONDITIONS
S11
GENERATE LEGITIMATE SIGNATURES
S12
REGISTER SUSPICIOUS SIGNATURE AND LEGITIMATE SIGNATURES IN FILTERING UNIT
S13
S14
IS PREDETERMINED THRESHOLD EXCEEDED?
NO
YES
S15
DOES NUMBER OF TIMES PREDETERMINED THRESHOLD IS CONTINUOUSLY EXCEEDED EXCEED PREDETERMINED VALUE?
NO
YES
SEND SUSPICIOUS SIGNATURE AND LEGITIMACY CONDITIONS TO ADJACENT REPEATER DEVICES
S16

FIG.8

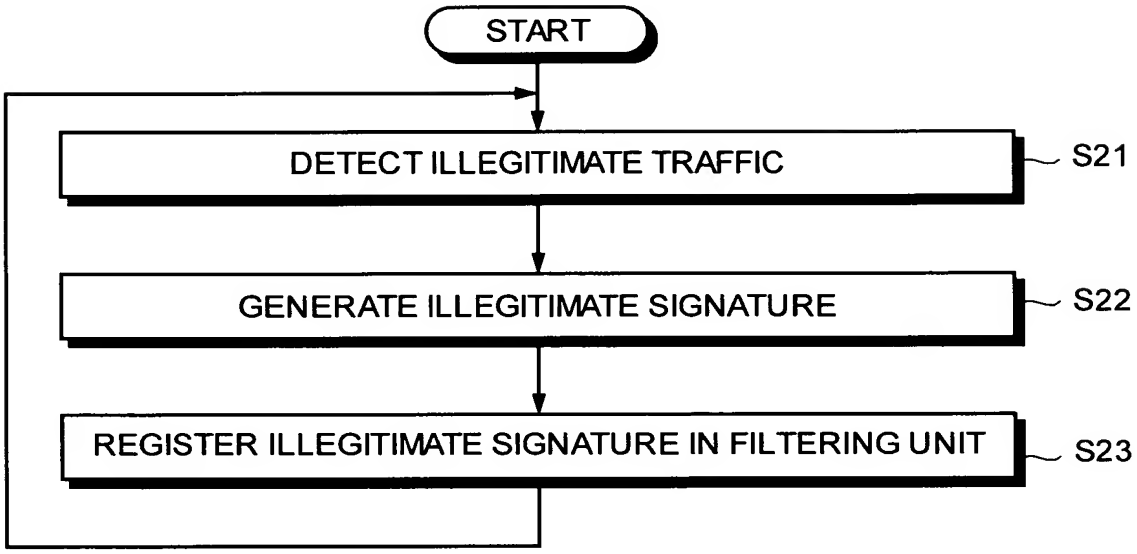

START
DETECT ILLEGITIMATE TRAFFIC
S21
GENERATE ILLEGITIMATE SIGNATURE
S22
REGISTER ILLEGITIMATE SIGNATURE IN FILTERING UNIT
S23

FIG.9

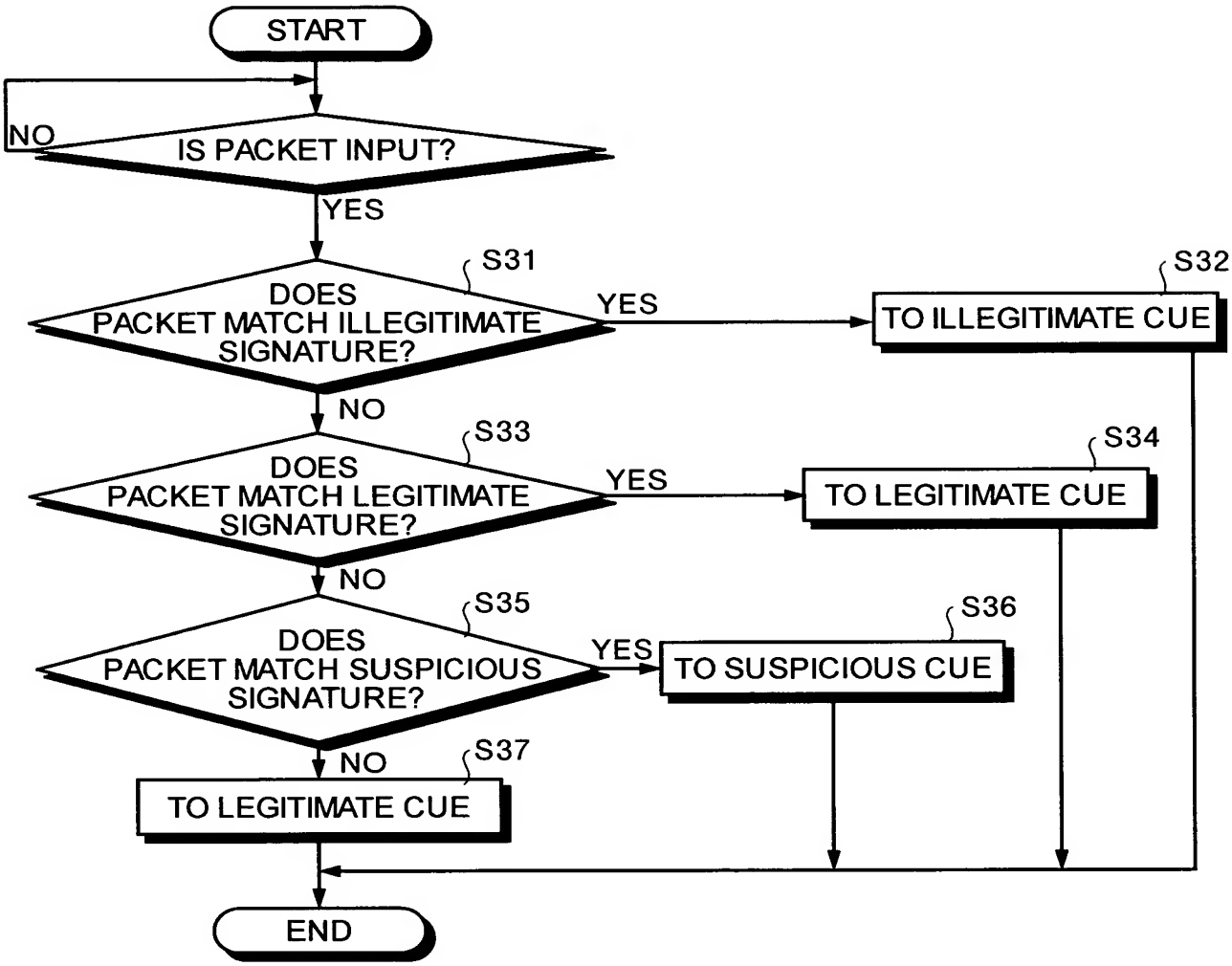

START
IS PACKET INPUT?
NO
YES
S31
DOES PACKET MATCH ILLEGITIMATE SIGNATURE?
YES
S32
TO ILLEGITIMATE CUE
NO
S33
DOES PACKET MATCH LEGITIMATE SIGNATURE?
YES
S34
TO LEGITIMATE CUE
NO
S35
DOES PACKET MATCH SUSPICIOUS SIGNATURE?
YES
S36
TO SUSPICIOUS CUE
NO
S37
TO LEGITIMATE CUE
END

FIG.10

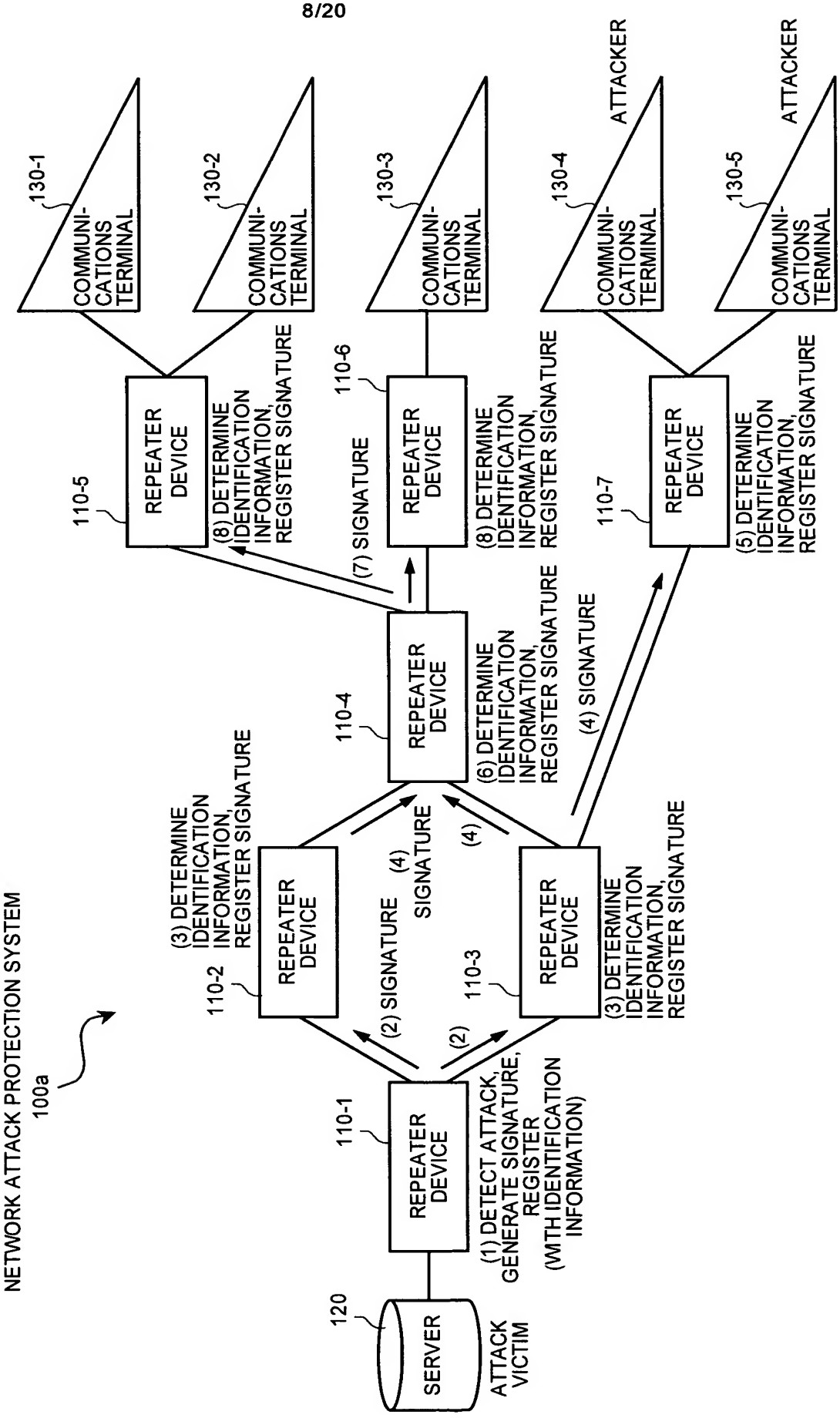

NETWORK ATTACK PROTECTION SYSTEM
100a
SERVER
120
ATTACK VICTIM
REPEATER DEVICE
110-1
(1) DETECT ATTACK, GENERATE SIGNATURE, REGISTER (MTH IDENTIFICATION INFORMATION)
110-2
110-3
110-4
110-5
110-6
110-7
(2) SIGNATURE
(2)
(3) DETERMINE IDENTIFICATION INFORMATION, REGISTER SIGNATURE
(4) SIGNATURE
(4)
(6) DETERMINE IDENTIFICATION INFORMATION, REGISTER SIGNATURE
(7) SIGNATURE
(8) DETERMINE IDENTIFICATION INFORMATION, REGISTER SIGNATURE
(5) DETERMINE IDENTIFICATION INFORMATION, REGISTER SIGNATURE
COMMUNICATIONS TERMINAL
130-1
130-2
130-3
130-4
130-5
ATTACKER

FIG.11

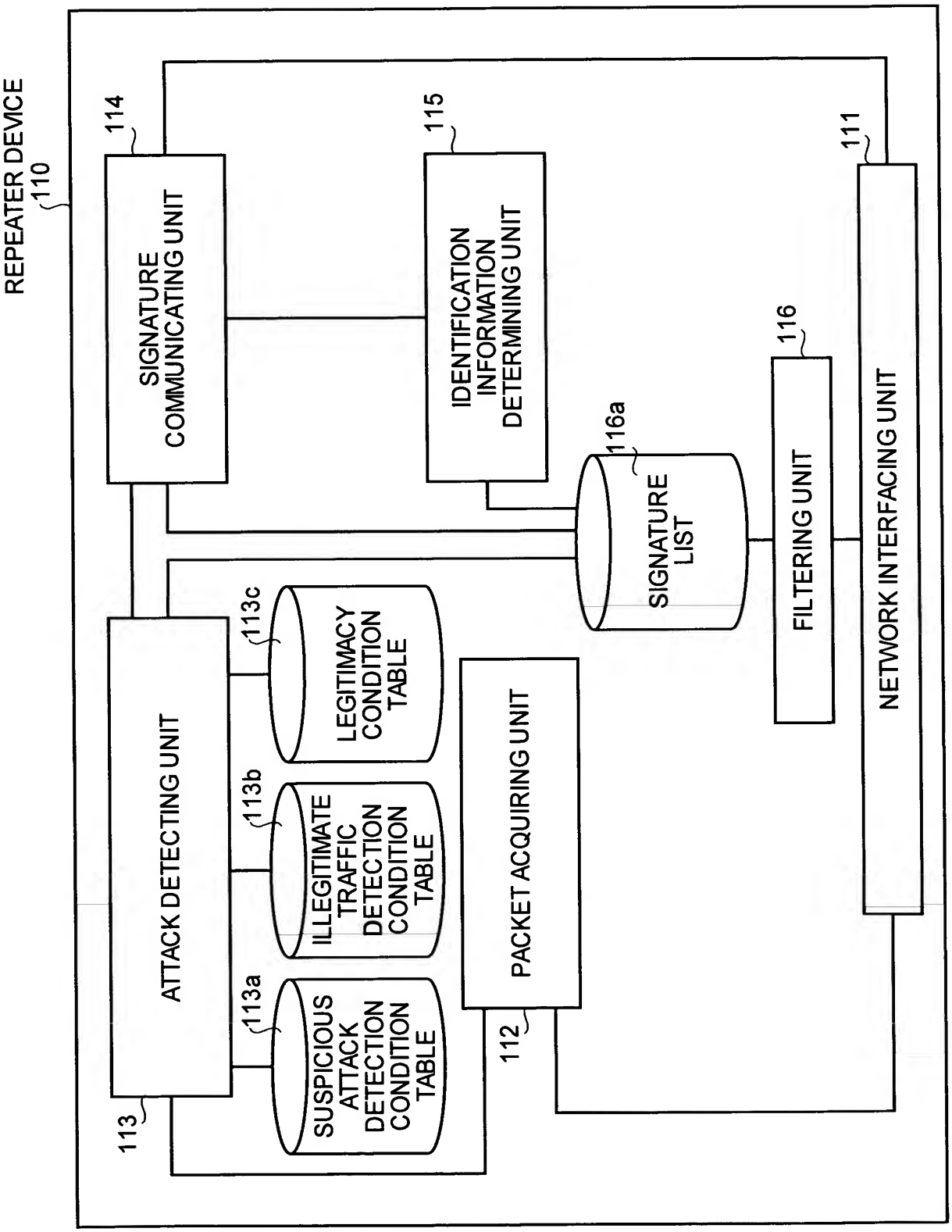

REPEATER DEVICE
110
SIGNATURE COMMUNICATING UNIT
114
IDENTIFICATION INFORMATION DETERMINING UNIT
115
NETWORK INTERFACING UNIT
111
FILTERING UNIT
116
SIGNATURE LIST
116a
ATTACK DETECTING UNIT
113
LEGITIMACY CONDITION TABLE
113c
ILLEGITIMATE TRAFFIC DETECTION CONDITION TABLE
113b
SUSPICIOUS ATTACK DETECTION CONDITION TABLE
113a
PACKET ACQUIRING UNIT
112

FIG.12

SUSPICIOUS ATTACK DETECTION CONDITION TABLE

113a

NO.	DETECTION ATTRIBUTES	DETECTION THRESHOLD	DETECTION TIME
1	{Dst=192.168.1.1/32,Protocol=TCP,Port=80}	500 Kbps	10 SECONDS
2	{Dst=192.168.1.2/32,Protocol=UDP}	300 Kbps	10 SECONDS
3	{Dst=192.168.1.1/24}	1000 Kbps	20 SECONDS
⋮			

FIG.13

ILLEGITIMATE TRAFFIC DETECTION CONDITION TABLE

113b

NO.	ILLEGITIMATE TRAFFIC CONDITIONS
1	PACKETS AT OR MORE ARE CONTINUOUSLY TRANSMITTED FOR S1 SECONDS OR MORE
2	ICMP/Echo Reply PACKETS AT T2 Kbps OR MORE ARE CONTINUOUSLY TRANSMITTED FOR S2 SECONDS OR MORE
3	FRAGMENT PACKETS AT T3 Kbps OR MORE ARE CONTINUOUSLY TRANSMITTED FOR S3 SECONDS OR MORE
⋮	

FIG.14

LEGITIMACY CONDITION TABLE

113c

NO.	DETECTION ATTRIBUTES
1	{Src=172.16.10.0/24}
2	{TOS=0×01}
⋮	

FIG.15

SIGNATURE LIST
116a

SIGNATURE	IDENTIFICATION INFORMATION	DOWNSTREAM NODE	UPSTREAM NODE
SIGNATURE A	(···,···,···,···)	REPEATER DEVICE 10-2	REPEATER DEVICE 10-5,10-6
SIGNATURE B	(···,···,···,···)	REPEATER DEVICE 10-3	REPEATER DEVICE 10-5,10-6
⋮	⋮	⋮	⋮

FIG.16

IDENTIFICATION INFORMATION
{LOCAL ALERT ID,ENGINE-TYPE,ENGINE-ID,NODE-ID}

- LOCAL ALERT ID:IDENTIFIER OF UNIQUE ALERT IN ANALYSIS ENGINE
- ENGINE-TYPE: IDENTIFIER OF ANALYSIS ENGINE TYPE
- ENGINE-ID: IDENTIFIER OF SAME ANALYSIS ENGINE BELONGING TO SAME MITIGATION
- NODE-ID: NODE IDENTIFIER OF MITIGATION TO WHICH ANALYSIS ENGINE BELONGS

FIG.17

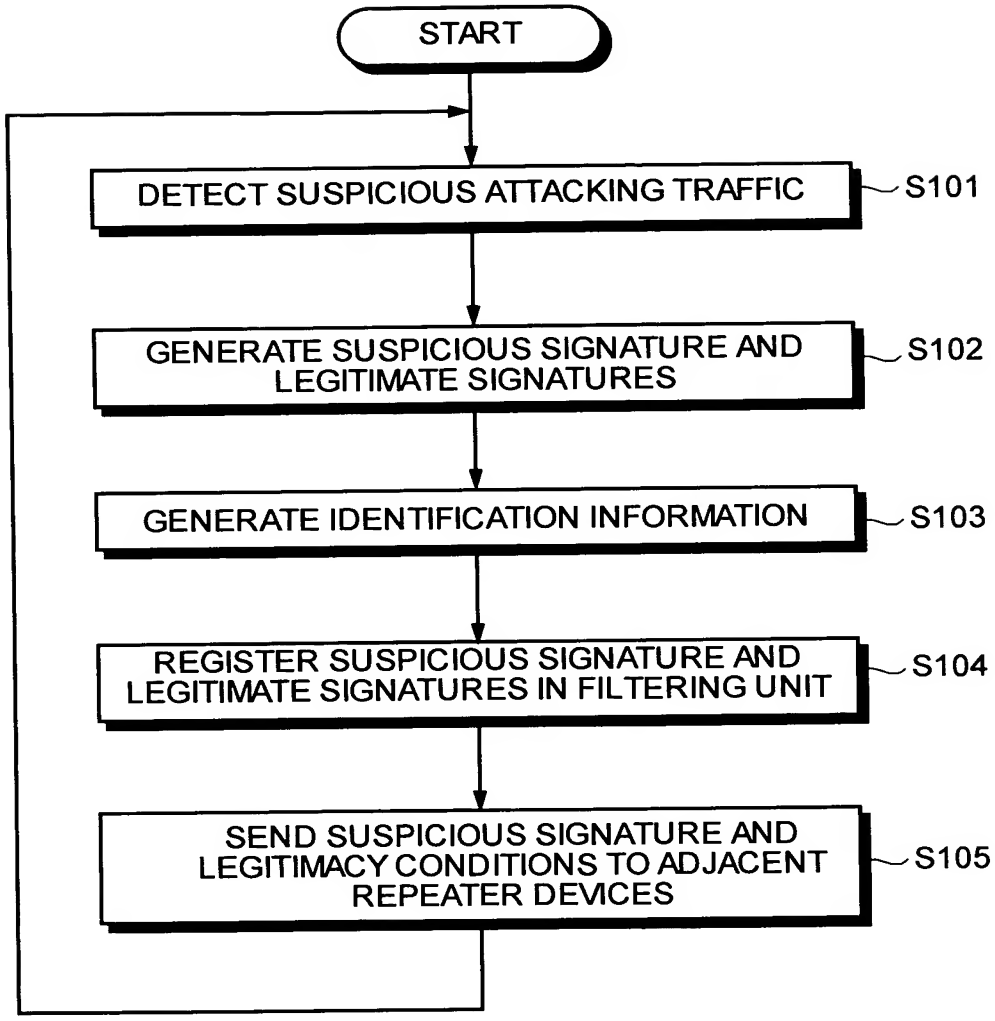

START
DETECT SUSPICIOUS ATTACKING TRAFFIC
S101
GENERATE SUSPICIOUS SIGNATURE AND LEGITIMATE SIGNATURES
S102
GENERATE IDENTIFICATION INFORMATION
S103
REGISTER SUSPICIOUS SIGNATURE AND LEGITIMATE SIGNATURES IN FILTERING UNIT
S104
SEND SUSPICIOUS SIGNATURE AND LEGITIMACY CONDITIONS TO ADJACENT REPEATER DEVICES
S105

FIG.18

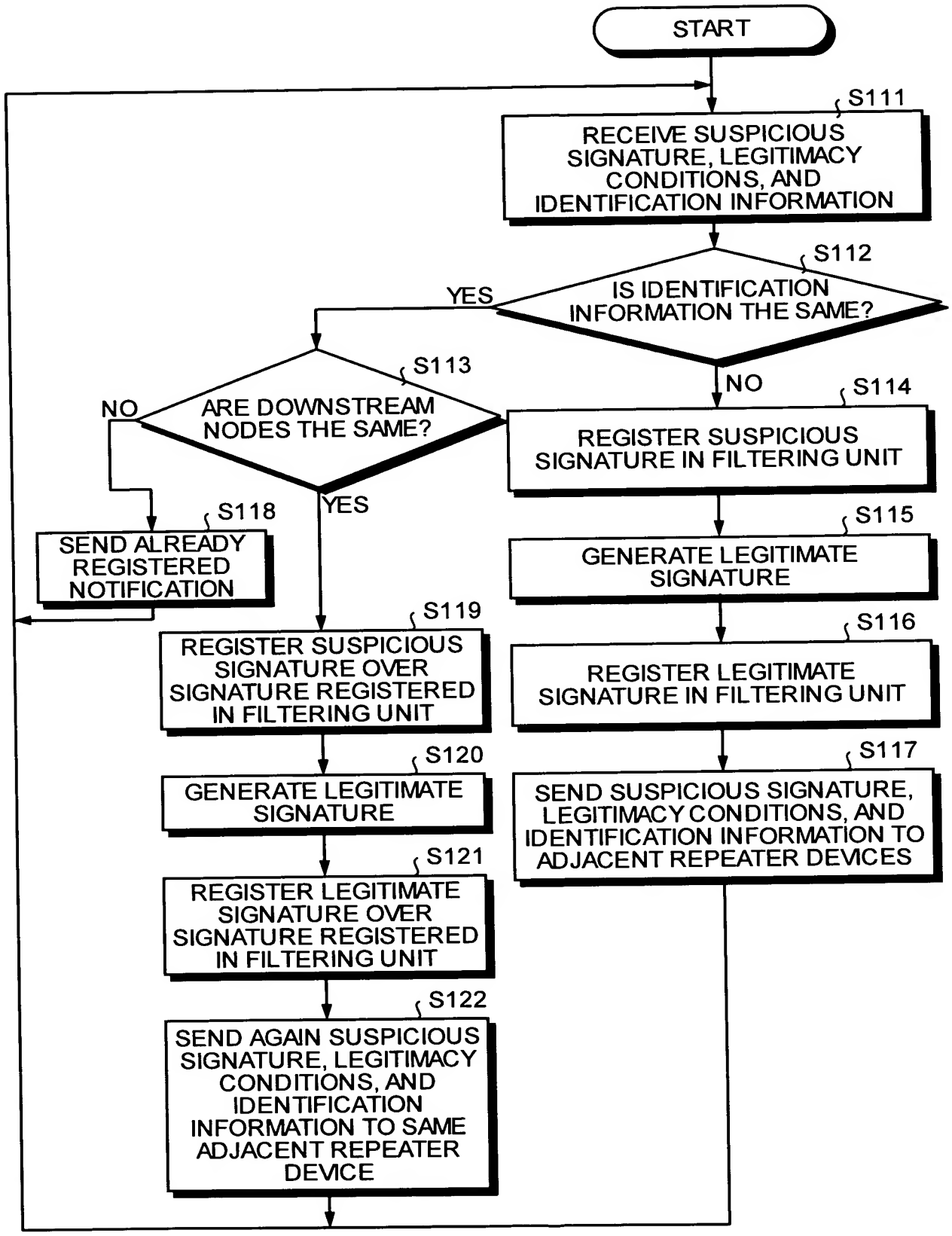

START
S111
RECEIVE SUSPICIOUS SIGNATURE, LEGITIMACY CONDITIONS, AND IDENTIFICATION INFORMATION
S112
IS IDENTIFICATION INFORMATION THE SAME?
YES
NO
S113
ARE DOWNSTREAM NODES THE SAME?
NO
YES
S114
REGISTER SUSPICIOUS SIGNATURE IN FILTERING UNIT
S115
GENERATE LEGITIMATE SIGNATURE
S116
REGISTER LEGITIMATE SIGNATURE IN FILTERING UNIT
S117
SEND SUSPICIOUS SIGNATURE, LEGITIMACY CONDITIONS, AND IDENTIFICATION INFORMATION TO ADJACENT REPEATER DEVICES
S118
SEND ALREADY REGISTERED NOTIFICATION
S119
REGISTER SUSPICIOUS SIGNATURE OVER SIGNATURE REGISTERED IN FILTERING UNIT
S120
GENERATE LEGITIMATE SIGNATURE
S121
REGISTER LEGITIMATE SIGNATURE OVER SIGNATURE REGISTERED IN FILTERING UNIT
S122
SEND AGAIN SUSPICIOUS SIGNATURE, LEGITIMACY CONDITIONS, AND IDENTIFICATION INFORMATION TO SAME ADJACENT REPEATER DEVICE

FIG.19

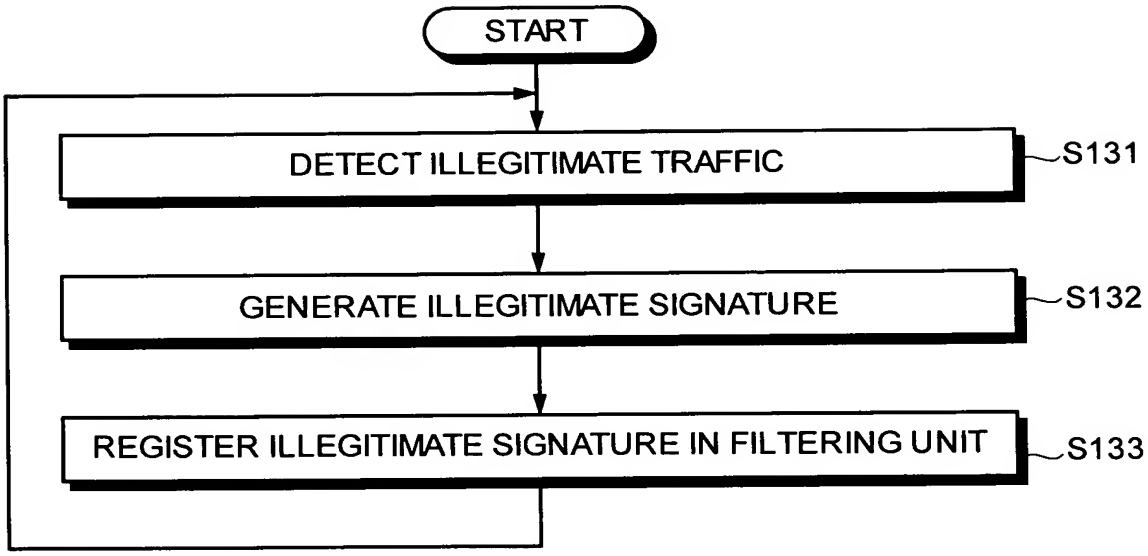

START
DETECT ILLEGITIMATE TRAFFIC
S131
GENERATE ILLEGITIMATE SIGNATURE
S132
REGISTER ILLEGITIMATE SIGNATURE IN FILTERING UNIT
S133

FIG.20

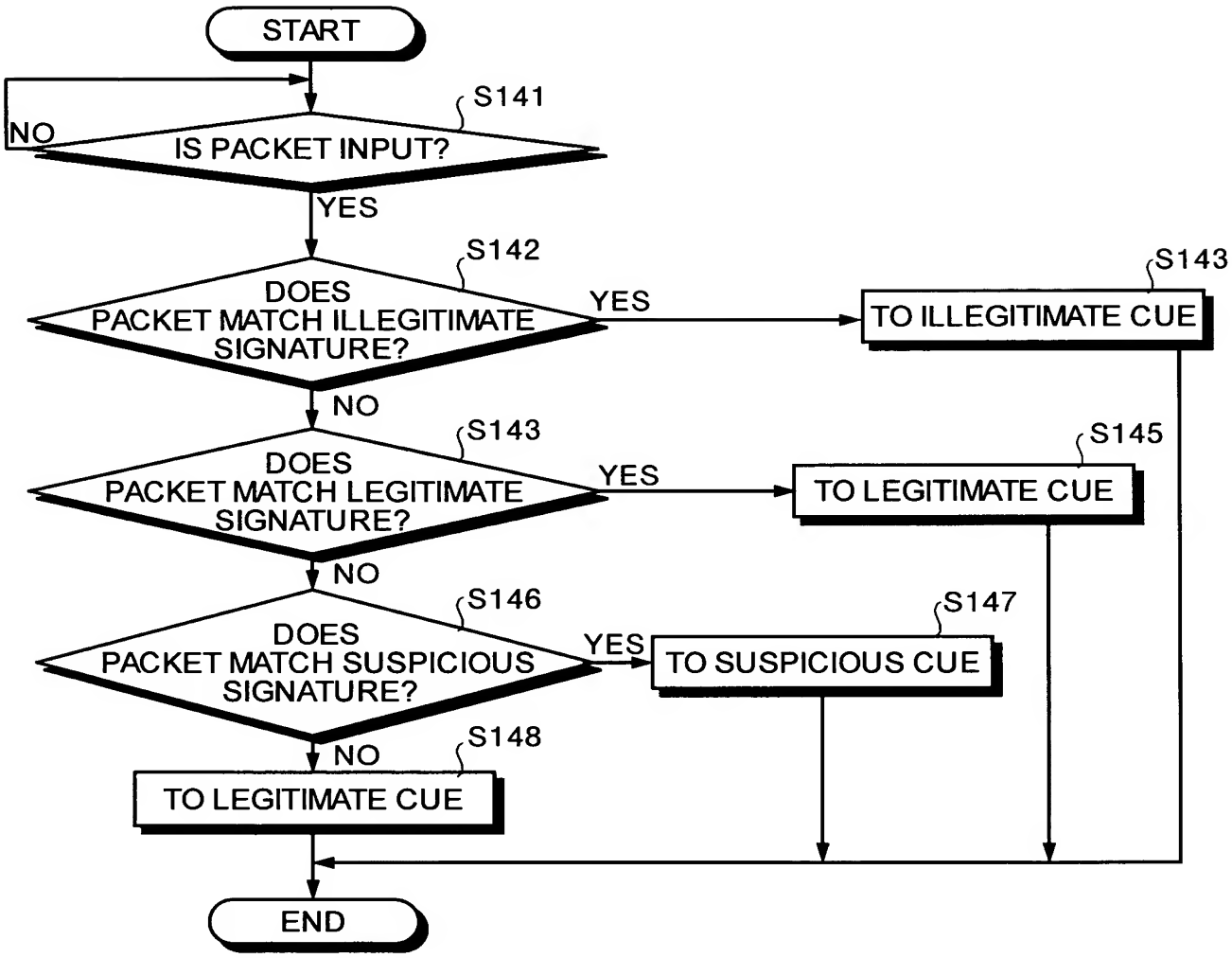

START
S141
IS PACKET INPUT?
NO
YES
S142
DOES PACKET MATCH ILLEGITIMATE SIGNATURE?
YES
S143
TO ILLEGITIMATE CUE
NO
S143
DOES PACKET MATCH LEGITIMATE SIGNATURE?
YES
S145
TO LEGITIMATE CUE
NO
S146
DOES PACKET MATCH SUSPICIOUS SIGNATURE?
YES
S147
TO SUSPICIOUS CUE
NO
S148
TO LEGITIMATE CUE
END

FIG.21

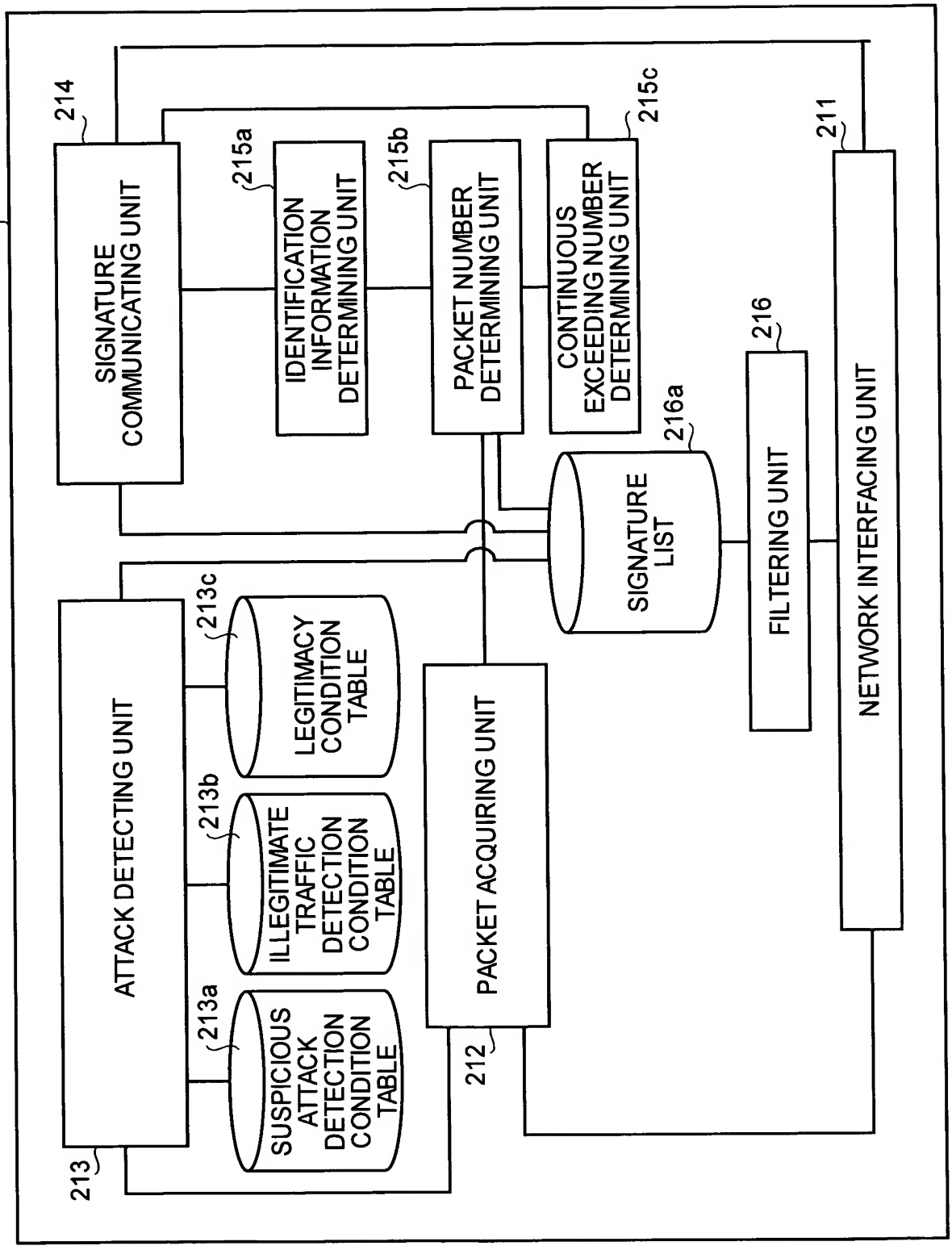

REPEATER DEVICE
210
214
SIGNATURE COMMUNICATING UNIT
215a
IDENTIFICATION INFORMATION DETERMINING UNIT
215b
PACKET NUMBER DETERMINING UNIT
215c
CONTINUOUS EXCEEDING NUMBER DETERMINING UNIT
211
NETWORK INTERFACING UNIT
216
FILTERING UNIT
216a
SIGNATURE LIST
213
ATTACK DETECTING UNIT
213a
SUSPICIOUS ATTACK DETECTION CONDITION TABLE
213b
ILLEGITIMATE TRAFFIC DETECTION CONDITION TABLE
213c
LEGITIMACY CONDITION TABLE
212
PACKET ACQUIRING UNIT

FIG.22

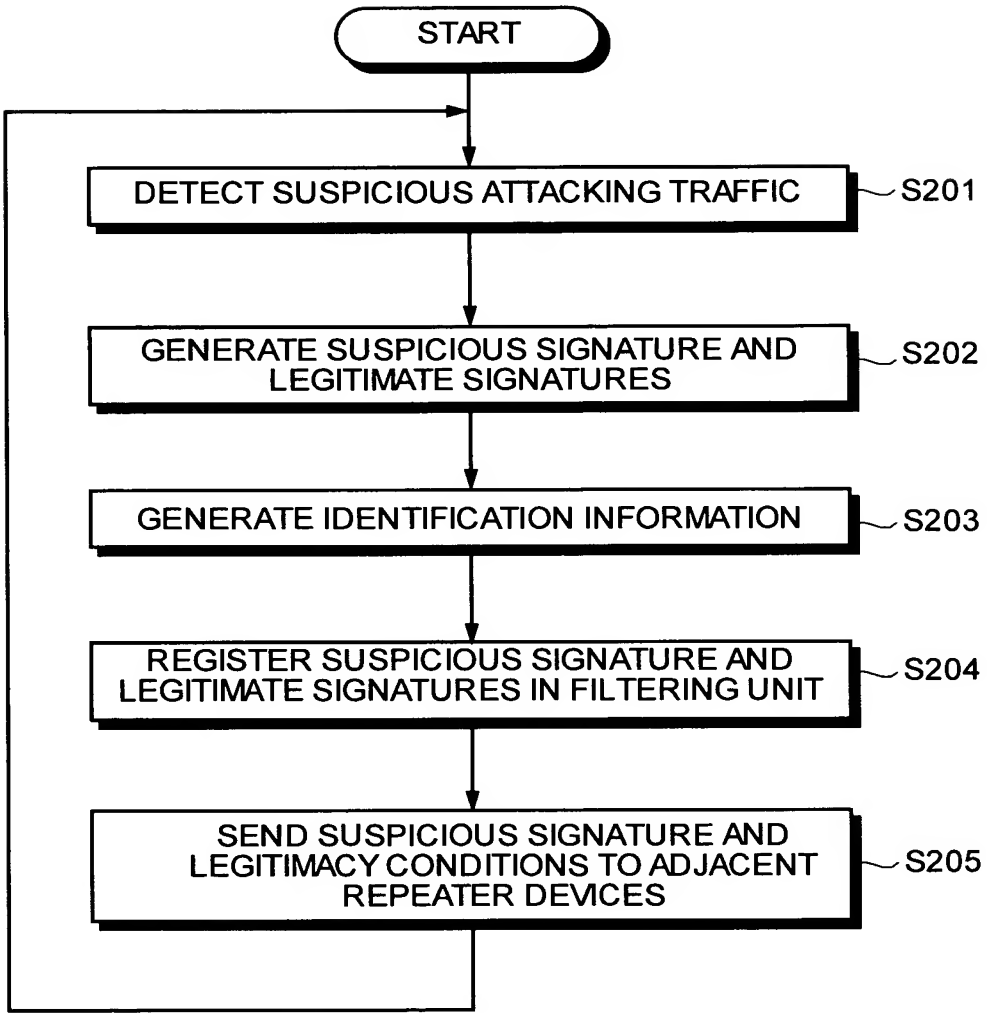

START
DETECT SUSPICIOUS ATTACKING TRAFFIC
S201
GENERATE SUSPICIOUS SIGNATURE AND LEGITIMATE SIGNATURES
S202
GENERATE IDENTIFICATION INFORMATION
S203
REGISTER SUSPICIOUS SIGNATURE AND LEGITIMATE SIGNATURES IN FILTERING UNIT
S204
SEND SUSPICIOUS SIGNATURE AND LEGITIMACY CONDITIONS TO ADJACENT REPEATER DEVICES
S205

FIG.23

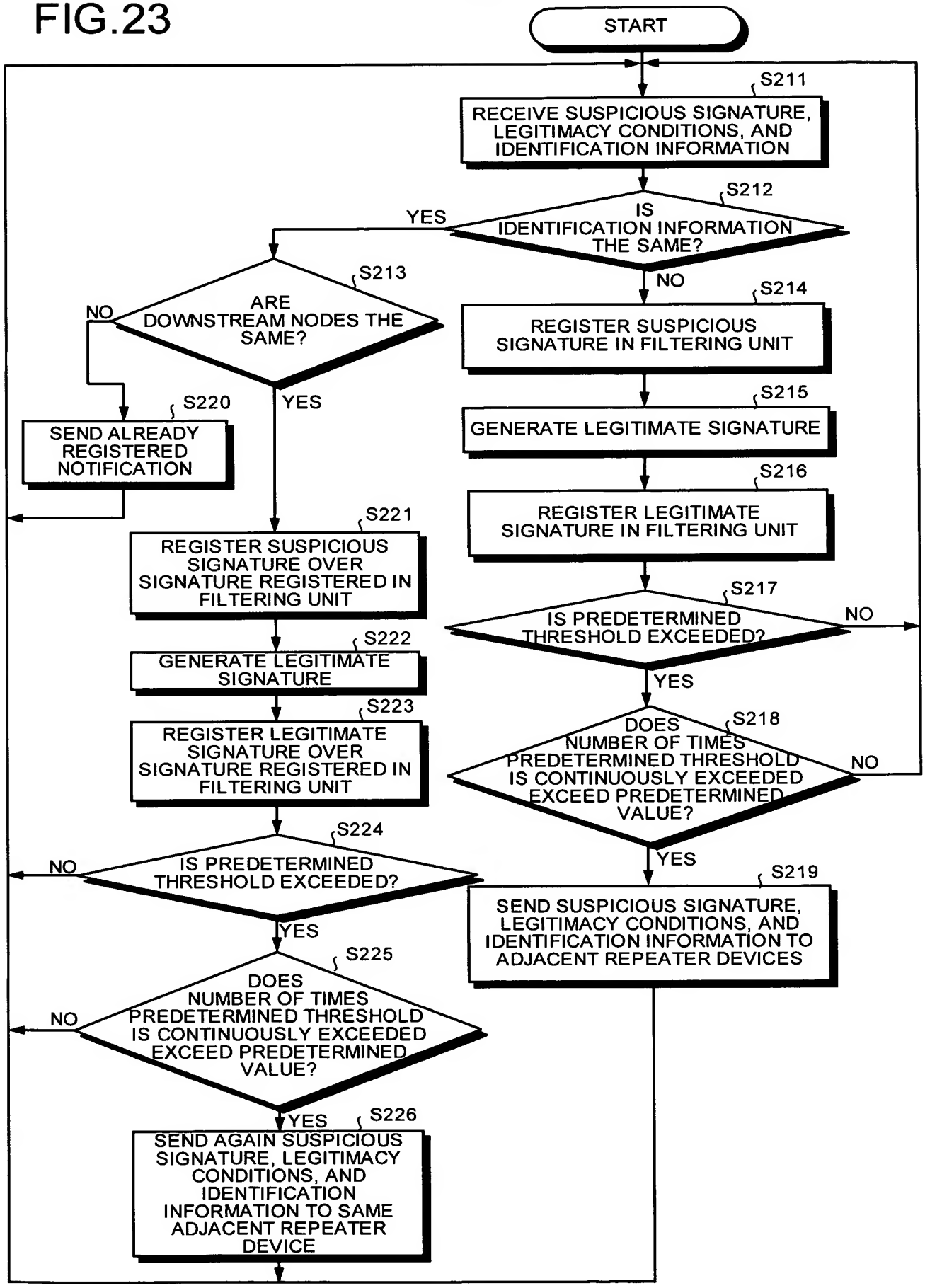

START
S211
RECEIVE SUSPICIOUS SIGNATURE, LEGITIMACY CONDITIONS, AND IDENTIFICATION INFORMATION
S212
IS IDENTIFICATION INFORMATION THE SAME?
YES
NO
S213
ARE DOWNSTREAM NODES THE SAME?
NO
YES
S214
REGISTER SUSPICIOUS SIGNATURE IN FILTERING UNIT
S215
GENERATE LEGITIMATE SIGNATURE
S216
REGISTER LEGITIMATE SIGNATURE IN FILTERING UNIT
S217
IS PREDETERMINED THRESHOLD EXCEEDED?
NO
YES
S218
DOES NUMBER OF TIMES PREDETERMINED THRESHOLD IS CONTINUOUSLY EXCEEDED EXCEED PREDETERMINED VALUE?
NO
YES
S219
SEND SUSPICIOUS SIGNATURE, LEGITIMACY CONDITIONS, AND IDENTIFICATION INFORMATION TO ADJACENT REPEATER DEVICES
S220
SEND ALREADY REGISTERED NOTIFICATION
S221
REGISTER SUSPICIOUS SIGNATURE OVER SIGNATURE REGISTERED IN FILTERING UNIT
S222
GENERATE LEGITIMATE SIGNATURE
S223
REGISTER LEGITIMATE SIGNATURE OVER SIGNATURE REGISTERED IN FILTERING UNIT
S224
IS PREDETERMINED THRESHOLD EXCEEDED?
NO
YES
S225
DOES NUMBER OF TIMES PREDETERMINED THRESHOLD IS CONTINUOUSLY EXCEEDED EXCEED PREDETERMINED VALUE?
NO
YES
S226
SEND AGAIN SUSPICIOUS SIGNATURE, LEGITIMACY CONDITIONS, AND IDENTIFICATION INFORMATION TO SAME ADJACENT REPEATER DEVICE

FIG.24

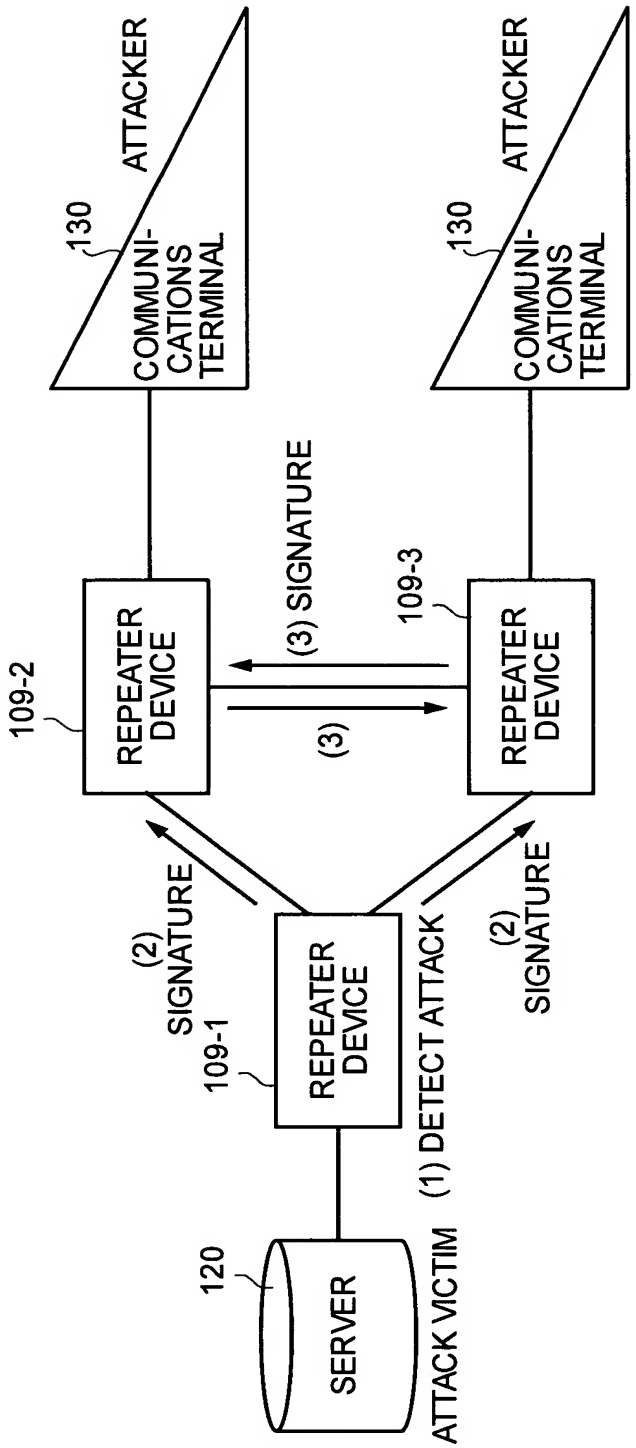
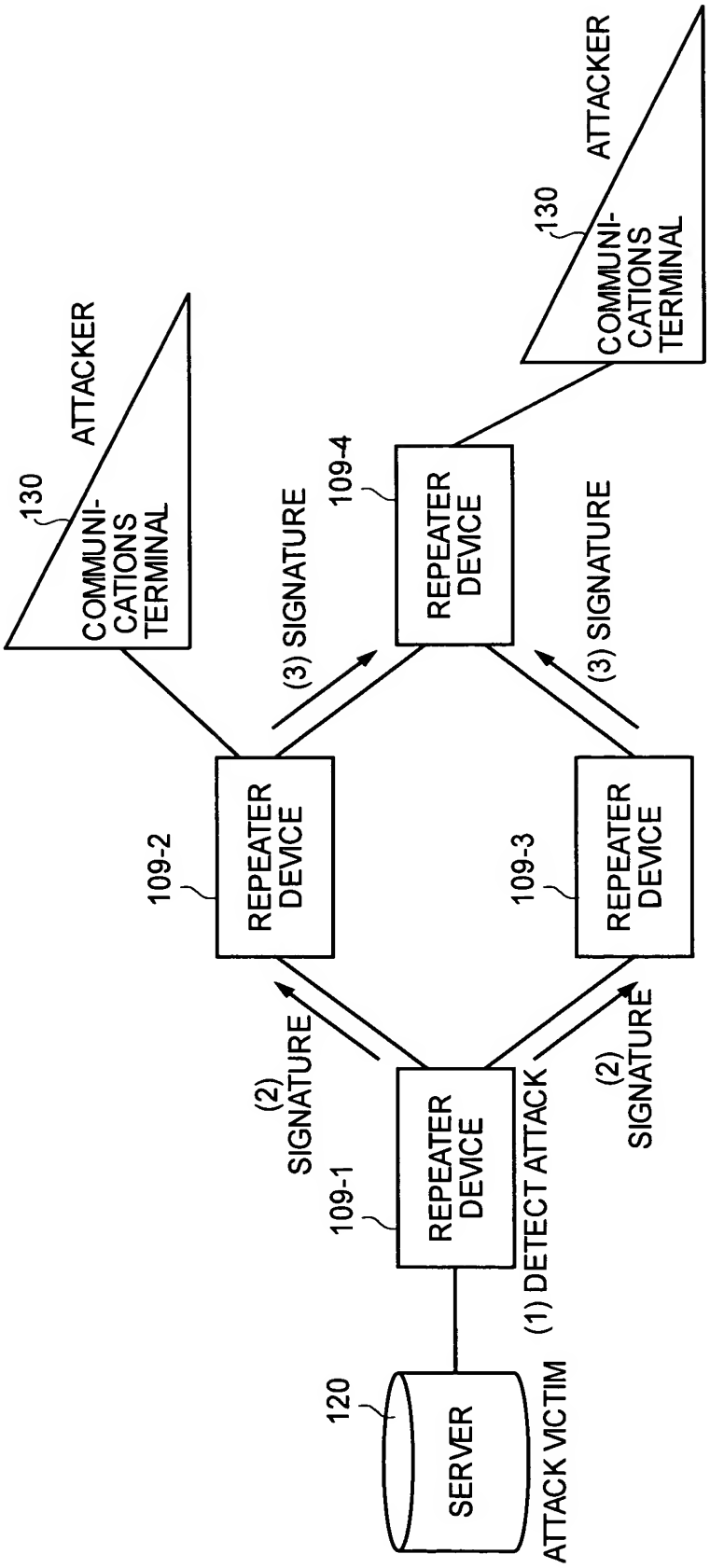

ATTACKER
130
COMMUNI-CATIONS TERMINAL
ATTACKER
130
COMMUNI-CATIONS TERMINAL
(3) SIGNATURE
109-3
109-2
REPEATER DEVICE
REPEATER DEVICE
(3)
(2) SIGNATURE
(2) SIGNATURE
109-1
REPEATER DEVICE
(1) DETECT ATTACK
120
SERVER
ATTACK VICTIM

FIG.25


ATTACKER
130
COMMUNI-
CATIONS
TERMINAL
ATTACKER
130
COMMUNI-
CATIONS
TERMINAL
109-4
REPEATER
DEVICE
(3) SIGNATURE
(3) SIGNATURE
109-2
REPEATER
DEVICE
109-3
REPEATER
DEVICE
(2)
SIGNATURE
(2)
SIGNATURE
109-1
REPEATER
DEVICE
(1) DETECT ATTACK
120
SERVER
ATTACK VICTIM